UNITED STATES OF AMERICA	)	
	)	**GOVERNMENT RESPONSE TO**
v.	)	**DEFENSE MOTION TO DISMISS**
	)	**SPECIFICATIONS 13 AND 14**
Manning, Bradley E.	)	**OF CHARGE II FOR FAILURE**
PFC, U.S. Army,	)	**TO STATE AN OFFENSE**
HHC, U.S. Army Garrison,	)	
Joint Base Myer-Henderson Hall	)	**24 May 2012**
Fort Myer, Virginia 22211	)	

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the defense motion to dismiss Specifications 13 and 14 of Charge II for failure to state an offense.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM), United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2008). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

The United States stipulates to the facts as set forth in the defense motion. The United States adds the following facts:

While deployed, the accused used two different Secret Internet Protocol Router Network (SIPRNET) computers: (1) a SIPRNET computer with the internet protocol (IP) address of 22.225.41.22; and (2) a SIPRNET computer with the IP address of 22.225.41.40. *See* Enclosure 1 at 126-27, 133. Before logging on to each computer with a username and password, the accused was presented with a warning banner. *See id.* at 134-35. The accused was required to click "OK" after being warned of the following:

> You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC, monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private,

> are subject to routine monitoring, interception and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g. authentication and access controls) to protect USG-interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the contect [sic] of priviledged [sic] communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement or details.

See id.; Enclosure 2.

During the Article 32 Investigation, the United States proceeded under the theory that because the accused's access to SIPRNET computers was governed by a purpose-based limitation or restriction, the accused exceeded authorized access when he accessed those classified government computers for an unauthorized or expressly forbidden purpose. *See* Enclosure 3. The purpose-based restriction was apparent in the first sentence of the warning banner, which notified the accused that he was "accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only." Enclosure 2; *see* Enclosure 1 at 134-35.

The accused and members of his unit were also required to sign a user agreement or acceptable use policy (AUP) prior to being granted access and a user network account (username and password) for the SIPRNET while deployed. *See* Enclosure 5. The Army's sample AUP states that "[a]ccess to this/these network(s) is for official use and authorized purposes…." *See* Enclosure 6 at 62. The purpose of an AUP is to obtain explicit acknowledgments from individuals on their responsibilities and limitations in using government information systems. *See id.* at 61.

Net-Centric Diplomacy

In response to the attacks of September 11th, Congress tasked the Office of the Director of National Intelligence to find a way to get key government agencies (e.g. Department of Defense (DOD) and Department of State (DOS)) to share information rapidly. *See* Enclosure 4. The Net-Centric Diplomacy Database (NCD), financed by DOD, was developed to provide a full range of diplomatic reporting ("diplomatic cables") to any individual with access to the DOD-controlled SIPRNET. *See id.* at 2. Diplomatic cables were routed to the NCD database or server, and thus made available to individuals with access to the SIPRNET, when the cable was assigned the code "SIPDIS" or "SIPR distribution." *See id.* at 3. In order for a SIPRNET user to access a diplomatic cable, the user must navigate through the SIPRNET to the NCD website (http://ncd.state.sgov.gov), and search the website for the desired cable.

WITNESSES/EVIDENCE

The United States requests this Court consider the following: (1) the referred charge sheet, (2) Enclosures 1-7, and (3) the Forensic Report for the accused's primary SIPRNET computer (BATES 00211066-00211069 or pp. 30-33 of the report).

LEGAL AUTHORITY AND ARGUMENT

The defense argues that the United States has failed to allege the accused "exceeded authorized access" within the meaning of 18 U.S.C. § 1030(a)(1). The defense argument has no merit. The Government's theory is that the accused "exceeded authorized access" when he violated the Government's explicit purpose-based access restriction on his SIPRNET computer. For the reasons set forth below, this theory of criminal liability under § 1030(a)(1) is consistent with the plain meaning of the statutory text, the legislative history, and case law interpreting the phrase "exceeds authorized access" in the context of prosecutions under § 1030.[1]

I. THE STATUTORY TEXT IS CLEAR AND UNAMBIGUOUS.

The defense claims the United States has failed to state an offense because, under the plain language of 18 U.S.C. § 1030(a)(1), the accused did not "exceed his authorized access." Def. Mot. at 4. The defense argument has no merit—the plain language of the statutory text clearly supports the Government's theory or interpretation of "exceeds authorized access."

The starting point for statutory interpretation is the plain or ordinary meaning of the language. *See United States v. McCollum*, 58 M.J. 323, 340 (C.A.A.F. 2003); *see also United States v. Custis*, 65 M.J. 366, 370 (C.A.A.F. 2007) ("[w]hen the statute's language is plain, the sole function of the courts…is to enforce it according to its terms"); 2A Sutherland Statutory Construction § 45:2 (7th ed.) ("a statute, clear and unambiguous on its face, need not and cannot be interpreted by a court"); *United States v. James*, 63 M.J. 217, 221 (C.A.A.F. 2006) ("a fundamental rule of statutory interpretation is that 'courts must presume that a legislature says in a statute what it means and means in a statute what it says there'") (citing *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992)). When a statute is clear and unambiguous, courts need not and should not consult the legislative history. *Ratzlaf v. United States*, 510 U.S. 135, 147-48 (1994) ("[W]e do not resort to legislative history to cloud a statutory text that is clear."); *see also United States v. Aleynikov*, 737 F. Supp. 2d 173, 177 (S.D.N.Y. 2010) ("When the statutory language is clear, there is no need to examine the statutory purpose, legislative history, or the rule of lenity.")

An individual "exceeds authorized access" under the Computer Fraud and Abuse Act (CFAA) and 18 U.S.C. § 1030(a)(1) when the individual "access[es] a computer with

[1] To the extent the United States did not clearly articulate its theory during oral argument on 23 February 2012, this brief , along with the theory presented during the Article 32 Investigation, should be considered the definitive source clarifying the Government's theory for "exceeding authorized access" on a SIPRNET computer.

authorization and...use[s] such access to obtain or alter information in the computer that the accesser is not entitled *so* to obtain or alter." 18 U.S.C. § 1030(e)(6) (emphasis added). The defense argues that a person exceeds authorized access only when he or she uses authorized access to a computer to obtain or alter information that he or she is never entitled to obtain or alter. *See* Def. Mot. at 3. The problem with this interpretation, however, is that the defense completely ignores the meaning of the word "so" in the definition.

"So" means "[i]n the state or manner indicated or expressed." *Webster's II New Riverside University Dictionary* 1102 (1988). The presence of "so" after "entitled" in § 1030(e)(6) makes the definition unambiguous—an individual "exceeds authorized access" when he or she obtains or alters information that he or she is not entitled to obtain or alter *in those circumstances.* Put another way, the word "so" clarifies that the user might have been entitled to obtain the information in *some other circumstances*, but not in that manner or under those circumstances. *See* 18 U.S.C. § 1030(e)(6) ("not entitled *so* to obtain or alter") (emphasis added). Thus, "exceeds authorized access" under § 1030(e)(6) clearly contemplates exceeding authorized access by violating an employer's purpose-based access restriction on a computer and obtaining information that, under those circumstances, the accused was not entitled to obtain.

The defense motion offers no explanation for Congress' decision to include the word "so" in the definition. In fact, they fail to mention the word completely when defining what constitutes "exceeding authorized access." *See* Def. Mot. at 5-6 ("A person exceeds authorized access under Section 1030(a)(1) when despite being authorized to use the computer, the accused uses his access to the computer to obtain or alter information in the computer that he is not entitled to obtain or alter.") ("An accused exceeds authorized access under Section 1030(a)(1) when, despite being authorized to use the *computer*, the accused uses his access to the computer to obtain or alter *information* in the computer that he is not entitled to obtain or alter."). Although the defense does not address the issue, the only conclusion that can be reached is that they consider the word "so" to be superfluous. To the extent the defense interpretation is that the term has no independent meaning or significance, this is improper. *See Corley v. United States*, 556 U.S. 303, 314 (2009) ("The fundamental problem with the Government's reading of [the statute] is that it renders [a provision] nonsensical and superfluous."). When a statute is construed, effect should be given to all its provisions so that no part is inoperative or superfluous. *Id.*

The statutory definition of "exceeds authorized access" is clear and unambiguous. The word "so" is not superfluous and was included in the definition by Congress for a reason. Accordingly, the defense motion should be denied because of the plain meaning of the statutory text.

II. THE LEGISLATIVE HISTORY SUPPORTS THE GOVERNMENT'S THEORY.

Assuming, *arguendo*, the statutory text is ambiguous, the relevant legislative history confirms the Government's interpretation of § 1030(a)(1) and "exceeds authorized access." In 1984, Congress enacted 18 U.S.C. § 1030 to address federal computer-related offenses in a single new statute. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,

Pub. L. No. 98-473, sec. 2102(a), 98 Stat. 1837 (1984). The 1984 version of 18 U.S.C. § 1030(a)(1) punished knowingly accessing a computer "without authorization," or accessing a computer with authorization and using the opportunity "such access provides for purposes to which such authorization does not extend...." *Id.* As evidenced by the language of the original statute, Congress clearly contemplated purpose-based restrictions on computer access, like the purpose-based restriction presented by the facts in this case. *See* Enclosure 2.

In 1986, Congress passed the "Computer Fraud and Abuse Act," which added to and amended 18 U.S.C. § 1030. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986). Specifically, the term "exceeds authorized access" was introduced to § 1030(a)(1) and (2). *Id.* at § 2(g)(6). As the Senate Report for the 1986 bill explained:

> Section 2(c) [of the 1986 bill] substitutes the phrase 'exceeds authorized access' for the more cumbersome phrase in present 18 U.S.C. § 1030(a)(1) and (2), 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend'. The Committee intends this change to simplify the language in 18 U.S.C. § 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in Section 2(g) of the bill.

S. Rep. No. 99-432, pt. 3, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.

In short, the Senate Report for the 1986 bill is clear—the phrase "exceeds authorized access" was substituted for the "more cumbersome phrase" in the 1984 version of 18 U.S.C. § 1030(a)(1). *Id.* Congress intended the change to "simplify the language in 18 U.S.C. § 1030(a)(1) and (2)," not wildly alter what type of conduct would be criminalized by the 1986 version of § 1030(a)(1). *Id.* Purpose-based restrictions, like those encompassed by the charged conduct in this case, continued to exist in the shorter and simpler phrase "exceeds authorized access."[2]

The defense asks this Court to scrutinize the section of the Senate Report entitled "Additional Views of Messrs. Mathias and Leahy." *See* Def. Mot. at 9; S. Rep. No. 99-432, pt. 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2493-96. Specifically, the defense cites to specific language from that section and argues that the "stated reason for the amendment was to 'eliminate coverage for authorized access that aims at purposes to which such authorization does not extend.'" Def. Mot. at 9 (quoting S. Rep. No. 99-432, pt. 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494). The defense fails to recognize that this section was devoted to a discussion of the scope of 18 U.S.C. § 1030(a)(3), not § 1030(a)(1) or (2). See S. Rep. No. 99-432, pt. 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494 (discussing the "three salutary features" of the revised § 1030(a)(3)). Senators Leahy and Mathias used this section to express their individual concerns that the 1984 version of § 1030(a)(3) encompassed "all computerized government information, including documents that must, under the Freedom of Information Act (FOIA), be

[2] Indeed, the defense notes that "[t]he language in the prior statute covered this situation perfectly; it criminalized the scenario where a person 'uses the opportunity that such [authorized] access provides for purposes to which such authorization does not extend.'" Def. Mot. at 9 (quoting Pub. L. No. 98-473, sec. 2102(a)).

disclosed to any member of the public upon proper request." S. Rep. No. 99-432, pt. 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494. The Senators believed the 1984 version of § 1030(a)(3) was "murky" because it potentially criminalized the conduct of a federal employee who, in response to a hypothetical FOIA request, accesses a computerized database without understanding the precise scope of their authorization. *See id.* As the Senators explained, a federal employee might resolve doubts about the scope of their authorization in those cases by refusing to disclose information under FOIA, "a conclusion directly contrary to the principles of open government underlying the FOIA." *Id.* The Senators' concerns were fully addressed by the 1986 bill, which restricted the scope of § 1030(a)(3) to punishing access to Government computers that occurred "without authorization." *See id.; see also* 18 U.S.C. § 1030(a)(3).

As evident from the record, Senators Mathias and Leahy did not believe the concept of exceeding authorized access was problematic, because they approved of a bill that preserved that basis for liability in § 1030(a)(1) and (2), and included it in a new provision, § 1030(a)(4). *See* 18 U.S.C. § 1030. They specifically recognized that a federal employee's "access to computerized data might be legitimate in some circumstances," but that in other circumstances, the employee "might be held to exceed his authorization." S. Rep. No. 99-432, pt. 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494-95. The Senators may have been concerned about imposing criminal liability on an individual for "exceeding authorized access" under § 1030(a)(3), but they had no similar concerns with respect to imposing liability under § 1030(a)(1), (2), and (4). Indeed, their discussion of the three "salutary" features of the revised § 1030(a)(3) acknowledged that other sections of 18 U.S.C. § 1030 would still be available to punish abuses of authorized access to federal computers. *See id.* ("As the committee report points out, administrative sanctions should ordinarily be adequate to deal with real abuses of authorized access to Federal computers (assuming of course, that no other provision of section 1030 is violated).").

The legislative history of the CFAA confirms that "exceeds authorized access" encompasses those individuals who access computer data in violation of an express purpose-based restriction on access. Senators Mathias and Leahy were abundantly clear that their concerns about the 1984 version of § 1030 were limited to the scope of § 1030(a)(3), and not § 1030(a)(1) and (2). *See id.* ("Among the many improvements that it would make is a complete revision of section 1030(a)(3).").

III. FEDERAL CASE LAW INTERPRETING "EXCEEDS AUTHORIZED ACCESS" SUPPORTS THE GOVERNMENT'S THEORY.

The Government's interpretation of "exceeds authorized access" is consistent with decisions from the Fifth and Eleventh Circuits, which have held that employees who violate clear company computer restriction agreements "exceed authorized access" under the CFAA. For example, in *United States v. John*, the Fifth Circuit held that an employee of Citigroup exceeded her authorized access in violation of § 1030(a)(2) when she accessed confidential customer information in violation of her employer's use restrictions and used that information to commit fraud. *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010). In *John*, the evidence demonstrated that the defendant was aware, through company training programs, of Citigroup's official policy prohibiting misuse of the company's internal computer systems and confidential

customer information. *Id.* As the Fifth Circuit noted, "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which the access has been given are exceeded." *Id.* Similarly, in *United States v. Rodriguez*, the Eleventh Circuit held that an employee of the Social Security Administration (SSA) exceeded his authorized access under § 1030(a)(2) when he obtained personal information about former girlfriends and potential paramours and used that information to send the women flowers or to show up at their homes. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2007). The evidence at trial showed that the SSA had established a policy that prohibited employees from obtaining information from its databases without a business reason. *Id.* at 1260. The SSA provided notice to employees through mandatory training sessions, notices posted in the office, and a banner that appeared on every computer screen daily. *Id.*

The reasoning of the Fifth and Eleventh Circuits is supported by the decisions of other courts as well. *See, e.g., Cont'l Group, Inc. v. KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1372 (S.D. Fla. 2009) (computer access policies stated that computers were provided "for business use" and were "to be used solely for the [authorizing party's] purposes"); *United States v. Salum*, 257 Fed. Appx. 225, 227 (11th Cir. 2007) (officers could access NCIC system only for official business of criminal justice agency); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 242-43, 248 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004) (in order to submit query to website, users must agree not to use responsive data for direct marketing activities); *United States v. Czubinski*, 106 F.3d 1069, 1071 (1st Cir. 1997) ("[IRS] employees may not use any Service computer system for other than official purposes.").

The defense asks this Court to adopt the interpretation of "exceeds authorized access" favored by the en banc Ninth Circuit Court of Appeals in *United States v. Nosal* (*Nosal III*), 2012 WL 1176119 (C.A.9 (Cal.)). *See* Def. Mot. at 12. *Nosal III* held that the phrase "exceeds authorized access" in the CFAA does not extend to violations of use or access restrictions. *Nosal III*, 2012 WL 1176119, at 7. However, *Nosal III* is seriously flawed for several reasons. First, while the majority acknowledged that the CFAA was "susceptible to the government's broad interpretation" of the statutory text, the court found the defendant's narrower version more plausible—and immediately launched into a parade of horribles that would ensue if the statutory text was given the government's interpretation. *See id.* at 3-6. In fact, the *Nosal III* majority spent much of the opinion considering scenarios not presented by the facts of the case—what the dissent called "far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy." *Id.* at 8 (Silverman, J., dissenting). As the dissent noted, the majority was preoccupied by the potential vagueness of other sections of the CFAA, when the majority should have "wait[ed] for an actual case or controversy to frame these issues, rather than posit a laundry list of wacky hypotheticals." *Id.* at 10 (Silverman, J., dissenting); *see also infra* Part V (discussing vagueness analysis).

Second, while the majority considered the narrower interpretation of the legislative history the "more sensible reading," they failed to seriously consider, beyond a short footnote, the legislative history with respect to Congress' intent to substitute a simpler phrase (exceeds authorized access) for "a more cumbersome phrase" in the 1984 version. *See id.* at 3; *see also supra* Part II (discussing the Senate Report for the 1986 bill). Instead, the majority simply stated that because one of the reasons for the 1984 bill was to address computer hacking, it is

"possible" to read both prohibitions ("without authorization" and "exceeding authorized access") as applying to hackers. *Nosal III*, 2012 WL 1176119, at 3. In the majority's view, "without authorization" would apply to "inside" hackers, and "exceeds authorized access" would apply to "outside hackers." *Id.* While the majority found this construction "plausible" or "possible," those words practically scream ambiguity. *See id.* Thus, the majority chose to neglect other methods of statutory interpretation, specifically legislative history, when led down that path by their own analysis.

Although the facts of the *Nosal* case are similar to those presented by this case, the other cases cited by the defense are not relevant to this Court's inquiry. *See* Def. Mot. at 6, 9, 11-12 (listing cases in support of the defense interpretation); *see also United States v. Nosal* (*Nosal II*), 642 F.3d 781, 782-83 (9th Cir. 2011) (summarizing facts of *Nosal*). As the *Nosal II* court noted, the defendant was subject to a computer use policy that placed clear and conspicuous restrictions on his access to the system and to a database in particular. *See id.* at 787. The other cases cited by the defense did not consider such explicit purpose-based restrictions or limitations on computer access. *See*, *e.g.*, *Aleynikov*, 737 F. Supp. 2d at 175 ("Among other things, Goldman employees were required to execute a confidentiality agreement...."); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 498 (D.Md. 2005) ("Defendant Werner-Matsuda signed a Registration Agreement stipulating not to use the information provided through VL lodge for any purpose that would be contrary to the policies and procedures established by the [IAM] Constitution."); *Walsh Bishop Assocs., Inc. v. O'Brien*, 2012 WL 669069, No. 11-2673 (DSD/AJB) (D.Minn. Feb. 28, 2012) ("Walsh Bishop argues that a person exceeds authorized access by accessing information in order to use it in a manner contrary to an employer's interests and use policies."); *Xcedex, Inc., v. VMware, Inc.*, 2011 WL 2600688, No. 10-3589 (PJS/JJK) (D.Minn. June 8, 2011). In short, the courts in the representative cases cited by the defense did not consider explicit purpose-based restrictions on computer access like this case and the *John* and *Rodriguez* cases.

This Court should reject the *Nosal III* interpretation of "exceeds authorized access" and adopt the reasoning of the Fifth and Eleventh Circuits. *Nosal III*, as source of precedent, is severely flawed. The majority improperly considered hypotheticals and scenarios not presented by the facts of the case and ignored relevant legislative history bearing on the issue. The other cases cited by the defense are not on point.

IV. RULE OF LENITY DOES NOT APPLY.

The defense argues that in cases where there are two possible interpretations of a statute – one broad and one narrow – courts should apply the rule of lenity and adopt the narrow interpretation. Def. Mot. at 20. Although the statutory text and legislative history are clear in this case and support the interpretation of the United States, the simple existence of some statutory ambiguity is not sufficient to warrant application of the rule of lenity. *Muscarello v. United States*, 524 U.S. 125, 138 (1998). Most statutes are ambiguous to some degree; thus the "mere possibility of articulating a narrower construction...does not by itself make the rule of lenity applicable." *Id.* (quoting *Smith v. United States*, 508 U.S. 223, 239 (1993)). The Supreme Court has stated that "the rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a 'grievous ambiguity or uncertainty in the statute,' such that the

Court must simply guess as to what Congress intended." *Barber v. Thomas*, 130 S. Ct. 2499, 2508-09 (2010) (quoting *Muscarello*, 524 U.S. at 139). In this case, there is no grievous ambiguity or uncertainty. If the Court is not convinced that "so" has independent meaning, the legislative history is clear on the issue of what interpretation to give "exceeds authorized access" in § 1030—Congress explained that the phrase was substituted for the "more cumbersome" phrase encompassing purposed-based restrictions. *See supra* Part II. In short, the problem posed by statutory interpretation in this case is no different from any other case. The rule of lenity does not stand for the proposition that the accused automatically wins in cases of ambiguity. *See Muscarello*, 524 U.S. at 139 ("Yet, this Court has never held that the rule of lenity automatically permits the defendant to win.")

V. THE ACCUSED DOES NOT HAVE STANDING TO RAISE VAGUENESS CHALLENGE.

Finally, the defense argues that the Government's "expansive interpretation" of "exceeds authorized access" puts a provision of § 1030 in constitutional jeopardy—specifically by rendering a sub-paragraph of § 1030(a)(2) void-for-vagueness. *See* Def. Mot. at 21-22. However, the accused is not charged with this allegedly vague provision. The only provision at issue in this case – § 1030(a)(1) – is also the only provision the accused may challenge for vagueness, as it is applied to him. *See Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 495 (1982) ("A [party] who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others."); *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2718-19 (2010) (quoting *Vill. of Hoffman*); *United States v. Kim*, 808 F. Supp. 2d 44, 52 (D.D.C. 2011) ("Defendant was not charged under the retention clause [of § 793(d)] and therefore he lacks standing to challenge it on vagueness grounds."). In short, the defense may not argue that a statutory interpretation renders an entirely different provision of § 1030 unconstitutionally vague, nor can he argue vagueness with respect to hypothetical applications of § 1030(a)(1). Void-for-vagueness challenges must be limited to the facts of the accused's own case. An interpretation of a phrase under § 1030(a)(1) that may lead to absurd results under another provision of § 1030 is irrelevant to the issues before this Court. Accordingly, this Court should decline to consider the defense arguments relating to vagueness.

CONCLUSION

The United States respectfully requests this Court DENY the defense motion to dismiss Specifications 13 and 14 of Charge II. For the reasons stated above, the United States has adequately stated an offense punishable under 18 U.S.C. § 1030(a)(1). In the alternative, the United States requests the Court either defer ruling on this motion until the presentation of evidence, or simply amend the specifications to leave the lesser-included offenses charging violations of clauses 1 and 2 of Article 134, Uniform Code of Military Justice.

JODEAN MORROW
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 24 May 2012.

JODEAN MORROW
CPT, JA
Trial Counsel

7 Encls
1. Article 32 Testimony of SA David Shaver
2. Accused's SIPRNET Warning Banner
3. Continuation Sheet, DD Form 457, pp. 29-32
4. Washington Post, dtd 31 Dec 12, *Cables Leak Reveals Flaws of Information-Sharing Tool*
5. AIR of SA Mander, dtd 5 Jan 11
6. Excerpt of AR 25-2, dtd 24 Oct 07
7. Accused's Non-Disclosure Agreements